

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

March 2, 2017

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Lexington Medical Center – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents Lexington County Health Services District, Inc., d/b/a Lexington Medical Center (“Lexington”). I write to provide notification concerning an incident that may affect the security of personal information of seven (7) New Hampshire residents. Lexington’s investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Lexington does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 13, 2017 Lexington Medical Center learned that it had been the target of a cyberattack. An unauthorized third party accessed Lexington’s employee information database, known as eConnect/PeopleSoft. This database contains personally identifiable information on current and former employees including names, birth dates, Social Security numbers and W-2 forms. When Lexington discovered this situation, it immediately eliminated further unauthorized access, promptly began an investigation and engaged several national cybersecurity firms to assist. Lexington also contacted federal and state law enforcement officials.

Lexington has devoted considerable time and effort to determine what exact information was contained on the database, and as such, may be at risk of disclosure. Lexington can confirm current and former employee names, birth dates, Social Security numbers and 2016 W-2 forms were included in the database. Importantly, the database does not contain any patient or employee spouse/dependent information.

To date, Lexington is not aware of any confirmed instances of identity fraud as a direct result of this incident. Nevertheless, Lexington wanted to make you (and the affected residents) aware of the incident and explain the steps Lexington is taking to help safeguard the residents against identity fraud. Lexington provided the New Hampshire residents with written notice of this incident commencing on March 3, 2017, in substantially the same form as the letter attached hereto. Lexington is offering the residents a **two year** complimentary membership with a credit

RECEIVED
OFFICE OF THE ATTORNEY GENERAL
MARCH 17 2017


Attorney General Michael A. Delaney
Office of the Attorney General
March 2, 2017
Page 2

monitoring and identity theft protection service. Lexington has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Lexington has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Lexington takes its obligation to help protect personal information very seriously. Lexington is continually evaluating and modifying its practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak

Encl.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

On February 13, 2017, we learned that Lexington Medical Center has been the target of a cyberattack. An unauthorized third party accessed our employee information database, known as eConnect/PeopleSoft.

The privacy of your information is very important to us. We want to notify you about this incident, explain the services we are making available to safeguard you against identity theft, and suggest steps that you should take.

What Happened?

An unauthorized third party accessed eConnect/PeopleSoft. This database contains personally identifiable information on current and former employees including names, birth dates, Social Security numbers and W-2 forms. A W-2 is a tax statement with your name, address, Social Security number, home address and information about your wages. **Importantly, the database does not contain any patient or employee spouse/dependent information.**

How Did We Respond?

Understandably, we became very concerned when we discovered this situation. We immediately eliminated further unauthorized access, promptly began an investigation and engaged several national cybersecurity firms to assist us. We also contacted federal and state law enforcement officials.

What Are We Doing Now?

We have established a dedicated and confidential call center staffed with identity theft professionals to help with any questions or concerns.

What Can You Do to Protect Your Personal Information?

Enclosed in this letter is information on enrolling in a free two-year membership for Experian's® ProtectMyID® Alert. There are also other precautionary measures you can take to protect your personal information, including setting up fraud alerts and a security freeze on your credit files, and obtaining a free credit report.

How Could Your Taxes Be Affected?

Your personal information from the W-2 may be used to file a fraudulent tax return. As a result, you should contact your tax advisor, if you have one, and let them know this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at [REDACTED] call the IRS at [REDACTED] to report the situation (the unit office is open Monday through Friday from 7:00 a.m. to 7:00 p.m.); and report the situation to your local police department. Additional information regarding preventing tax-related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>. *Additional instructions for filing the affidavit (Form 14039) are included on the following pages.*

What Are Some Ways You Can Recognize Identity Theft with Your Tax Records?

- Your attempt to file your federal tax return was rejected.
- You receive a notice from the IRS indicating someone else was using your Social Security number.

How Can You Get More Information?

If you have further questions regarding this incident, please call our dedicated and confidential call center at [REDACTED]. The call center is open Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. If you call after hours, leave a message and someone will return your call.

We are committed to safeguarding your information by dedicating resources to help you resolve any issues related to this situation.

It's disheartening that we live in a world where this kind of violation can happen to hard-working, compassionate health care professionals. I understand this situation is very frustrating, but we will get through it together.

Sincerely,

[REDACTED]
[REDACTED]

**- OTHER IMPORTANT INFORMATION -
HOW TO PROTECT YOUR PERSONAL INFORMATION**

Protecting your personal information is important to Lexington Medical Center. Here are some ways to help protect yourself from fraud or identity theft.

Enroll in Free 24-Month Credit Monitoring

In response to a recent cyberattack at Lexington Medical Center, the hospital has arranged for you to enroll in Experian's® ProtectMyID® Alert for a two-year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's ProtectMyID in Three Easy Steps:

1. ENSURE that you enroll by [REDACTED]
2. VISIT the ProtectMyID website to enroll: [REDACTED]
3. PROVIDE your nine-character activation code: [REDACTED]

If you have questions or need an alternative to enrolling online, please call [REDACTED]

Additional Details Regarding Your 2-Year ProtectMyID Membership:

A credit card is not required for enrollment. Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies.
 - Identity theft can happen months or years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of fraud resolution support after your ProtectMyID membership expires.

Once you complete your enrollment in ProtectMyID, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [REDACTED]

Place a Free Fraud Alert

Whether you choose to use the complimentary 24-month credit monitoring service, we recommend that you place an initial 90-day fraud alert on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
Equifax.com
(800) 525-6285

Experian
P.O. Box 2002
Allen, TX 75013
Experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
TransUnion.com
(800) 680-7289

Consider Placing a Security Freeze on Your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request that a security freeze be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit file by sending a request in writing, by mail, to **all three** nationwide credit reporting companies. To learn more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
Freeze.Equifax.com
(800) 525-6285

Experian Security Freeze
PO Box 9554
Allen, TX 75013
Experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
TransUnion.com/securityfreeze
(800) 680-7289

If you decide to place a Security Freeze on your credit file, in order to do so without paying a fee you will need to provide a police report. If your personal information has been used to file a false tax return or to open an account or to attempt to open an account, you may file a police report in the City in which you currently reside.

Obtain a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from **each** of the above three major nationwide credit reporting companies. Call **(877) 322-8228** or request your free credit reports online at **AnnualCreditReport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors you did not authorize. Verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Make Use of Additional Helpful Resources

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts.

You may also file a complaint with the FTC by contacting them online at FTC.gov/idtheft, by phone at (877) IDTHEFT or (877) 438-4338, or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC, 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you live in **Iowa**, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General
Consumer Protection Division
1305 East Walnut Street
Des Moines, IA 50319
(515) 281-5164
1-888-777-4590
Fax: (515) 281-6771
www.iowaattorneygeneral.gov

If you live in **North Carolina**, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Instances of known or suspected identity theft should also be reported to law enforcement.

If you live in *Maryland*, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Report Identity Fraud to the IRS

If you believe you are a victim of identity fraud and it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was using your Social Security number, it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS. (Download the form at IRS.gov/pub/irs-pdf/f14039.pdf.)**
 - *Instructions for Form 14039* – In Section A, check box 1. In Section B, check box 2. Insert this information in the “Please provide an explanation” box: *My company informed me that a third party unlawfully obtained certain employee personal information including my W-2.*
- Call the IRS at (800) 908-4490, ext. 245, to report the situation. The unit office is open Monday through Friday from 7:00 a.m. to 7:00 p.m.
- Contact your tax preparer, if you have one.
- Call or visit your local law enforcement agency and file a police report. Please bring the letter from your employer with you.

Additional information regarding preventing tax-related identity theft can be found at IRS.gov/uac/Identity-Protection

Report Identity Fraud to the Social Security Administration

If you believe you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at (800) 772-1213 or visit Secure.SSA.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security statement on SocialSecurity.gov/myaccount.

The Social Security Administration has published *Identity Theft and Your Social Security Number* online at SSA.gov/pubs/EN-05-10064.pdf.